The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
09/17/2012

09/18/2012 – UPDATED

SUBJECT:
Vulnerability in Internet Explorer Could Allow Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. Exploitation may occur if a user visits or is redirected to a web page which is specifically crafted to take advantage of the vulnerability. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.
It should be noted that there is currently no patch available for this vulnerability and it is currently being exploited in the wild resulting in remote code execution. In addition, the exploit code is currently available as a Metasploit module.

September 18 UPDATED OVERVIEW
Microsoft has released a workaround for this vulnerability in Security Advisory 2757760.

SYSTEMS AFFECTED:

- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9

September 18 UPDATED SYSTEMS AFFECTED:

- ***Internet Explorer 6***

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:

A vulnerability has been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. The vulnerability occurs due to Internet Explorer improperly handling a condition where a deleted object is accessed. This may result in a use-after-free condition and lead to execution of arbitrary code. A use-after-free condition occurs when an application de-allocates a memory block and then later attempts to access that de-allocated space.
Exploitation may occur if a user visits or is redirected to a web page which is specifically crafted to take advantage of this vulnerability. Successful exploitation of the vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in adenial-of-service condition.

It should be noted that there is currently no patch available for this vulnerability and it is currently being exploited in the wild resulting in remote code execution. In addition, the exploit code is currently available as a Metasploit module.

September 18 UPDATED OVERVIEW
Microsoft has released a workaround for this vulnerability in Security Advisory 2757760. By default Internet Explorer on Windows Server 2003, Windows Server 2008, and Windows Server 2008 R2 runs in a restricted mode that is known as Enhanced Security Configuration. Microsoft has indicated that this mitigates the vulnerability on those systems.

RECOMMENDATIONS:
The following actions should be taken:

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- If you have an alternate browser deployed, consider using it until this vulnerability is remediated.

September 18 – UPDATED RECOMMENDATIONS:
The following workarounds from Microsoft be taken:

- ***Deploy the Enhanced Mitigation Experience Toolkit***
- ***Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones***
- ***Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone***

REFERENCES:
SecurityFocus:
http://www.securityfocus.com/bid/55562

ZDNet:
http://www.zdnet.com/java-zero-day-leads-to-internet-explorer-zero-day-7000004330/

AlienVault:
http://labs.alienvault.com/labs/index.php/2012/new-internet-explorer-zero-day-being-exploited-in-the-wild/

September 18 UPDATED REFERENCES

Microsoft:

http://technet.microsoft.com/en-us/security/advisory/2757760

http://blogs.technet.com/b/msrc/archive/2012/09/17/microsoft-releases-security-advisory-2757760.aspx